



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER OF PATENTS AND TRADEMARKS  
Washington, D.C. 20231  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/202,024	08/25/1999	FRANK SCHAEFER-LORINSER	2345/45	2371

26646 - 7590 03/31/2003

KENYON & KENYON  
ONE BROADWAY  
NEW YORK, NY 10004

EXAMINER

HUSEMAN, MARIANNE

ART UNIT PAPER NUMBER

3621

DATE MAILED: 03/31/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

**Office Action Summary**

Application No.

09/202,024

Applicant(s)

SCHAEFER-LORINSER ET AL.

Examiner

M. Huseman

Art Unit

3621

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 16 January 2003.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 15 - 29 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 15-29 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☒ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 16 January 2003 is/are: a) ☐ accepted or b) ☒ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- 11) ☐ The proposed drawing correction filed on \_\_\_\_\_ is: a) ☐ approved b) ☐ disapproved by the Examiner.
- If approved, corrected drawings are required in reply to this Office action.
- 12) ☐ The oath or declaration is objected to by the Examiner.

**Priority under 35 U.S.C. §§ 119 and 120**

- 13) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- \* See the attached detailed Office action for a list of the certified copies not received.
- 14) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).
- a) ☐ The translation of the foreign language provisional application has been received.
- 15) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

**Attachment(s)**

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) \_\_\_\_\_
- 4) ☐ Interview Summary (PTO-413) Paper No(s). \_\_\_\_\_
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other:

### DETAILED ACTION

1. The drawings are objected to as failing to comply with 37 CFR 1.84(p)(5) because they include the following reference sign(s) not mentioned in the description: elements "130", "132", "134", "136", "138" and "140" of figure 3. A proposed drawing correction, corrected drawings, or amendment to the specification to add the reference sign(s) in the description, are required in reply to the Office action to avoid abandonment of the application. The objection to the drawings will not be held in abeyance.
2. The drawings are objected to under 37 CFR 1.83(a). The drawings must show every feature of the invention specified in the claims. Therefore, the "input data", chip card and security module of claim 15 must be shown or the feature(s) canceled from the claim(s). Also, a drawing illustrating that an additional feedback is tapped off following a first of the at least one second downstream counter and before the latch as claimed in claim 25. This also applies to the limitation claimed in claim 26. Further, the second of the at least one second downstream counter of claim 27 must be shown or the feature(s) canceled from the claim(s). There is also no figure illustrating an XOR circuit as claimed in claim 28. No new matter should be entered.

A proposed drawing correction or corrected drawings are required in reply to the Office action to avoid abandonment of the application. The objection to the drawings will not be held in abeyance.

### ***Claim Rejections - 35 USC § 112***

3. The following is a quotation of the first paragraph of 35 U.S.C. 112:  

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.
4. Claims 20 and 24 – 29 are rejected under 35 U.S.C. 112, first paragraph, as containing subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention.

Regarding claim 20:

It is not clear as to where in the specification there is disclosure for selecting the first number of clock pulses to enable calculating of an authentication token to be based on a second number of clock pulses as claimed in claim 20.

Regarding claims 24 – 29:

The specification contains "exemplary embodiments", none of which are specific to a particular inventive device; i.e., the terms "may", "or", "at least one" and "for example" are used to describe a number of embodiments. There appears to be no "preferred embodiment" (definitive elements that would make up Applicants' inventive device) within the specification. Therefore, it is not clear as to what Applicants' consider to be their invention. See 37 CFR § 1.71.

Regarding claim 25:

There is no description in the specification of a "latch".

5. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

6. Claims 18 and 24 – 29 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

In claim 18, there is no proper antecedent basis for "different contents". There is also no proper antecedent basis for "in calculating an authentication token"; i.e., a positive recitation of a step for calculating an authentication token is missing from the claim (this also applies to claim 20).

In claim 24, line 6, the term -first- should be inserted before "counter".

In claims 25 - 28, there is no proper antecedent basis for "the additional feedback".

#### ***Claim Rejections - 35 USC § 103***

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the

invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

8. Claims 15 – 23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Chaum et al '238.

Regarding claims 15, 21 - 23:

Chaum et al teach a multi-purpose transaction card system such that Applicants' step of debiting a requested cash amount from the chip card reads on the card of Chaum et al and Applicants' step of adding and storing the requested cash amount in a summing counter reads on the secure application module of Chaum et al, column 56, lines 29 – 38.

Although Chaum et al do not specifically describe Applicants' steps of subdividing, loading, introducing and switching (random generator), Chaum et al do disclose that any random generator may be used to provide the cryptographic computations. Further, Applicants' appear to be stating in their remarks (paper #14, page 2) that their generator (i.e., LFSR, counter, clock and switch) is "conventional". Therefore, it is considered that it would have been obvious to one of ordinary skill in the art at the time of the invention to utilize any combinations of shift registers, counters, clocks and switch to form a generator as a matter of design choice.

Regarding claims 16 and 17:

Chaum et al disclose that the input data (to the terminal/module from the card) includes a random number (column 12, lines 38 – 51), a secret key/signature (column 20, lines 13 – 19 and columns 25 - 26, lines 46 – 67 and 1 – 3, respectively), and non-secret chip card data ("town result value").

Regarding claims 18 and 19:

Chaum et al disclose a counter and counters inherently will count to 1.

***Claim Rejections - 35 USC § 102***

9. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Art Unit: 3621

10. Claims 24 and 29 are rejected under 35 U.S.C. 102(b) as being anticipated by Koopman, Jr. et al '270.

Koopman, Jr. et al, figures 2a and 2b, teach cryptographic authentication of transmitted messages using pseudorandom numbers such that Applicants' first counter reads on element 38 (64 bit word), Applicants' linear feedback shift register reads on elements 108 and 109 and column 6, lines 19 – 42, Applicants' additional non-linear feedback shift register reads on either elements 113 and 115 or elements 116 and 114, column 6, lines 19 – 42, and Applicants' limitation of the register being disconnectable reads on the operation of the clocks 117 and 118.

### **Conclusion**

11. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. Menezes et al, "Handbook of Applied Cryptography", Chapter 6, disclose stream ciphers utilizing LFSRs and non-linear FSRs. Goode discloses a ciphering system utilizing nonlinear feedback shift registers.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to M. Huseman whose telephone number is 703-605-4277. The examiner can normally be reached on Monday - Friday, 6:30 AM - 3:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, James Trammell can be reached on 703-305-9768. The fax phone numbers for the organization where this application or proceeding is assigned are 703-305-7687 for regular communications and 703-305-7687 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-308-1113.

  
JAMES P. TRAMMELL  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 3800



M. Huseman  
Examiner  
Art Unit 3621

mh  
March 24, 2003